〔論　説〕

アメリカのプライバシー保護法制の日本への示唆

牧　田　潤　一　朗

Ⅰ　はじめに

本稿は，筆者が，2008 年度日弁連客員研究員留学制度（米国カリフォルニア大学バークレー校ロースクールへ派遣）により行ったプライバシーに関する研究内容の一部をまとめたものである。

アメリカでは，プライバシー概念が早くから提唱され，これに対する判例上，立法上の措置が取られてきた。しかし，多くの努力にも関わらず，日本と同様，プライバシー保護に多くの課題を残している。これらの課題は，日本のプライバシー保護立法を検討する上で有益な示唆を含んでいるものと考える。したがって，本稿では，アメリカにおけるプライバシー保護の歴史を概観した上で，プライバシー保護に関する連邦法を紹介し，アメリカにおけるプライバシー保護の課題と日本への示唆を検討することとした。

Ⅱ　アメリカのプライバシー保護の歴史[1)]

アメリカ連邦法には，日本の「個人情報の保護に関する法律」（以下「個人情報保護法」という）に相当する個人情報保護[2)]の一般法は存在せず，特定の分野毎に個別の立法が多数存在する，いわゆるセクトラル方式の個人情報保護となっている。ここでは，アメリカのプライバシー保護の歴史を概観し，個別立法がなされるようになった経緯と重要な個別立法例を紹介する。

１　ウォーレン＆ブランダイス論文

1890 年，弁護士であったサミュエル・D・ウォーレンとルイス・D・ブランダイスが「プライバシーの権利」（The Right to Privacy）という論文を執筆し，この論文が事実上アメリカのプライバシー保護の出発点となった。同論文は，ジャーナリズムの台頭と簡便なカメラといった新技術の登場により，「ひとりにしておいてもらえる権利」（The right to be let alone）としてのプライバシー侵害の危険が増大した状況を指摘し，プライバシーを暴かれ，精神的苦痛を受けた者は，コモンローにより保護されるべきであると説いた[3)]。1900 年代初頭から裁判所と

---

1) 日本の文献としては，堀部政男『プライバシーと高度情報化社会』22 頁以下（岩波新書，1988 年），阪本昌成『プライヴァシー権論』245 頁以下（日本評論社，1986 年），石井夏生利『個人情報保護法の理念と現代的課題』121 頁以下（勁草書房，2008 年）。

2) 個人情報保護とプライバシー保護は，厳密には異なるものであるが，ここでは，個人情報保護をプライバシー保護のための手段と捉える。

3) Samuel D. Warren & Louis D. Brandeis, “The Right to Privacy”, *HARV. L. REV*, 4 (1890) p.193.

立法府は，不法行為により，同論文が主張する精神的苦痛の救済を図るようになる[4)]。

２　不法行為法上のプライバシーの発展[5)]

不法行為法上のプライバシー侵害訴訟が増加したことを受けて，1960 年，ウィリアム・プロッサー教授は，プライバシー侵害訴訟を調査し，これを①私事への侵入（Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs），②私事の公開（Public disclosure of embarrassing private facts about the plaintiff），③公衆の誤認（Publicity which places the plaintiff in a false light in the public eye），④氏名又は肖像の盗用（Appropriation, for the defendant's advantage, of the plaintiff's name or likeness）の 4 類型に分類した[6)]。現在，この 4 類型は整備され，リステイトメントに採用されている[7)]。各分類の特徴を表にまとめると以下のとおりである。不法行為訴訟におけるプライバシー侵害の主張は，専らこれら 4 類型を構成する事実を主張することになる。これらは, 排他的ではなく, 1 つの事件で重複して主張されることが多い。

表 1

	秘匿性	公　表	内容の誤り	侵害者の利得
私事への侵入	必要	不要	不要	不要
私事の公開	必要	必要	不要	不要
公衆の誤認	不要	必要	必要	不要
盗　用	不要	不要 （通常有）	不要	必要

4) Daniel J. Solove & Paul M. Schwartz, *Information Privacy Law*, 3rd ed., 2008, pp.25-26.
5) 日本の文献としては，石井・前掲注 1）150 頁以下参照。
6) William Prosser, "Privacy", *CALIF. L. REV.* 48 (1960) p.383.
7) RESTATEMENT (SECOND) OF TORTS, 2nd ed., AMERICAN LAW INSTITUTE PUBLISHERS, 1977, §652B-E. なお，リステイトメントとは，「アメリカ法の主要分野のうち判例を中心に発達した諸領域をとりあげ, 法域によって立場が異なる点については, その内容を検討し, 法域の数よりも当該準則の合理性を重視しつつ取捨選択し, これを条文の形にまとめ, かつ説明（comment）と例（illustration）を付したもの. …（略）…法源としての拘束力はないが, 実際に当事者により, また裁判所によってよく引用され, 間接的にではあるがアメリカ法の統一に一定の役割を果たしている.」（田中英夫編『英米法辞典』（東京大学出版会，1991 年））。

(1)私事への侵入

リステイトメントでは，「物理的その他の手段で，他人の孤独若しくは隔離状態又は他人の私的事項に，意図的に侵入した者は，その侵入が，思慮分別ある一般人から見て甚だしく不快な場合には，プライバシーの侵害として責任を負う」とされている[8)]。

侵入は，家の中といった私的空間だけに限られない。公共の場においても問題となりうる。自動車の危険性を告発した消費者保護活動家ラルフネーダーに対して，自動車製造会社が人を雇って，彼の私的事項を探索した等の主張がされた事件で，ニューヨーク州控訴裁判所は，特定の個人について単なる情報収集をすることは不法行為上の侵入に該当しないが，秘密とされている情報の収集について思慮分別ある一般人から見て相当でない侵入態様である場合にはプライバシー侵害に該当するとした。その上で，公共の場で行為したからといってその全てを公開しているわけではなく，人を尾行して調査し続けることは，執拗に行われた場合には不法行為になりうると判示した[9)]。

(2)私事の公開

リステイトメントでは，「他者の私的生活事項を公開した者は，当該事項の公開が，思慮分別ある一般人から見て甚だしく不快である場合，かつ公共の正当な関心事でない場合には，プライバシーの侵害として責任を負う」とされている[10)]。

私的生活事項かどうかは，情報の性質，情報が存在する場所の性質（原則として，公共の領域にある情報は，私的な事項には該当しない），開示態様（任意か否か），事前の開示範囲（誰が知っていたか）等が考慮される[11)]。公開は，原則として，広範囲へ情報が開示された場合に認められるが，情報の性質等によっては，ごく限られた範囲での開示でも認められる[12)]。

[8)] RESTATEMENT (SECOND) OF TORTS, 2nd ed., §652B.
[9)] Nader v. General Motors Corp., 255 N.E.2d 765 (N.Y. Ct. App. 1970).
[10)] RESTATEMENT (SECOND) OF TORTS, 2nd ed., §652D.
[11)] *See*, Gill v. Hearst Publishing Co., 253 P. 2d 441 (Cal. 1953), Daily Times Democrat v. Graham 162 So. 2d 474 (Ala. 1964), McNamara v. Freedom Newspapers, Inc., 802 S.W. 2d 901 (Tex. Ct. App. 1991), Times Mirror Co. v. Superior Court, 244 Cal. Rptr. 556 (Cal. Ct. App. 1988).
[12)] 例として，乳房切断手術の事実を同僚に開示した雇用主に対する損害賠償請求が認められた事案がある（Miller v. Motorola, Inc., 560 N.E. 2d 900 (Ill. App. 1990)）。

私事の公開は，報道の自由と鋭く対立する。この利益調整として報道価値の審査（Newsworthiness Test）が行われる。リステイトメントの注釈では，「当該公表行為が，公衆の受領すべき情報の提供を止め，自己のための病的で煽情的な覗きとなり，思慮分別ある公衆が，適正な規範に照らし，それについて関心がないと言う場合」に報道価値がないとされている[13]。有名な事例として，大統領暗殺をたまたま現場に居合わせて阻止し全米のヒーローとなった一般人について，後日，同性愛者であったと報道されたことがプライバシー侵害になるか問題となった事件がある。判決は，同人が積極的に同性愛保護団体の活動に参加しており，同性愛者である事実は私的事項ではないこと，及び報道の目的は，同性愛者が臆病で軟弱な人間であるという誤った一般の意見を払拭することにあって報道価値が認められることなどを認定し，プライバシー侵害を認めなかった[14]。現在の多くの裁判例は，報道価値の判断にあたり，当該個人と公共の利益との間に何らかの関連性を要求する（Nexus Test）。公的人物であれば，報道価値は認められやすいが，認められない場合もありうる[15]。報道価値の要件は，報道目的をどのように構成するかによってほとんどいかなる報道も正当化しうるとの指摘もある。

私事の公開による不法行為の成立については，さらに表現の自由を定める合衆国憲法修正 1 条からの制約がある。連邦最高裁は，1975 年，報道機関が起訴状に記載されていたレイプ被害者の氏名を報道した事件に関し，一旦閲覧できる公の裁判書類として真実の情報が明らかにされた時は，その報道によって報道機関が罰を受けることはないと判示して，レイプ被害者の氏名等の開示を犯罪としていたジョージア州法を違憲とした[16]。また，1979 年にも，少年犯罪者の氏名の出版を禁じたウエストバージニア州法について，新聞社が合法に取得した公共的な真実の情報である場合，その報道を禁止するのは，より重要な州

---

[13] RESTATEMENT (SECOND) OF TORTS, 2nd ed., § 652D, comment h.
[14] Sipple v. Chronicle Publishing Co., 201 Cal. Rptr. 665 (Cal. Ct. App. 1984).
[15] 地域の大学で最初の女性の学生自治会長となった人物について，性同一性障害であることの報道に報道価値があるか問題とされた事件で，裁判所は，原告に性同一性障害があることが彼女の当該役職における誠実さや判断能力にどのような悪影響を与えるかその関連性はほとんど見いだせないとして，報道価値の有無を判断するため陪審手続段階へ進むことを認め，サマリージャッジメント（正式事実審理を経ない判決）を認めなかった（Diaz v. Oakland Tribune, 188 Cal. Rptr. 762 (Ct. App. 1983)）。
[16] Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).

の利益がなければ，違憲であると判示した[17)]。さらに，1989 年には，性犯罪被害者の名前の出版，放送等を違法とするフロリダ州法に違反して新聞社が被害者の名前を報道したため提起された民事損害賠償請求訴訟において，警察の報告から得た性犯罪被害者の名前を報道したことに関して新聞社への損害賠償請求を認めることは合衆国憲法修正 1 条違反であるとした[18)]。

このようにプライバシー保護目的の報道規制は，報道内容に着目した規制となるため，厳格な審査基準で判断されている。

(3) 公衆の誤認

リステイトメントでは，「公衆の誤認をもたらす他者の事実を公表した者は，その誤認が，思慮分別ある一般人から見て甚だしく不快な場合で，行為者が公表事実の誤りについて知りつつ又は全く注意を怠って行動した場合には，プライバシーの侵害として責任を負う」とされている[19)]。

公衆の誤認は，名誉毀損（defamation）と類似するが，名誉毀損が社会的評価の低下を問題にするのに対し，公衆の誤認は，直接精神的苦痛を問題とする[20)]。ただし，両者は，同一の事案で重複して主張することが可能である。また，合衆国憲法修正 1 条からの制約として，連邦最高裁は，1967 年，公の人物に関する報道に関する誤りについては，名誉毀損と同様に現実の悪意の法理（Actual Malice standard）[21)]を採用し，不法行為の成立を制限している[22)]。

表 2

	名誉毀損	公衆の誤認
損　害	社会的評価の侵害を要する	もっぱら精神的苦痛
不快の程度	不　要	甚だしく不快

17) Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979).
18) The Florida Star v. B.J.F. 491 U.S. 524 (1989).
19) RESTATEMENT (SECOND) OF TORTS, 2nd ed., § 652E.
20) 表現の自由への制約を増大させる懸念から名誉毀損とは別に公衆の誤認という不法行為を認めない州裁判所もある（*See*, Lake v. Wal-Mart Stores, Inc., 582 N.W. 2d 231 (Minn. 1998)）。
21) 名誉毀損の成立を行為者が公表事実の誤りについて知りつつ又は全く注意を怠って行動した場合のみに限る法理。*See*, New York Times Co. v. Sullivan, 376 U.S. 254 (1964).
22) Time, Inc. v. Hill, 385 U.S. 374 (1967).

(4) 盗　用

リステイトメントでは，「自己の利用又は利益のため，他者の氏名や肖像を盗用した者は，プライバシーの侵害として責任を負う」とされている[23]。

これは，自己の名前や肖像に表わされる個人の利益（社会的評価，経済的地位，公共的価値その他）を独占的に本人が利用する利益を保護したものと説明されている[24]。類似の概念として，パブリシティ権[25]があり，その区別として，盗用は精神的損害を保護し，パブリシティ権は財産的損害を保護するという説明もされている[26]。しかし，リステイトメントでは，盗用について，精神的損害は重要な要素だが，その性質は財産権であるとされており[27]，その区別は必ずしも明確ではない。

3　憲法上のプライバシー権

プライバシー侵害の不法行為訴訟が増加する中，1960 年中頃から 1970 年中頃にかけて，プライバシーは，社会的な関心の中心となっていた。この時期，電子盗聴が重要な社会問題となり，また，1965 年，連邦政府が，その持っている個人情報を統合するナショナル・データ・センター設立を提言したことは，大きな社会的反発を引き起こし，連邦議会でも意見聴取が行われた末に，廃案となった。

このような時期に，連邦最高裁は，1965 年グリズウォルド対コネティカット判決[28]において，避妊具の使用及び避妊方法について結婚した夫婦に助言・指導することを処罰するコネティカット州法を夫婦間のプライバシーの権利を侵害するものとし，アメリカ合衆国憲法上明文を欠くプライバシーの権利を憲法上の権利として初めて認めた。また，1977 年のワーレン対ロー判決[29]において，

---

[23] RESTATEMENT (SECOND) OF TORTS, 2nd ed., §652C.
[24] *Id*., comment a, c.
[25] RESTATEMENT (THIRD) OF UNFAIR COMPETITION, AMERICAN LAW INSTITUTE PUBLISHERS, 1995, §46.
[26] J. Thomas McCarthy, *The Right of Publicity and Privacy*, 2nd ed., West Group, 2003, §5:61, p.5-110.
[27] RESTATEMENT (SECOND) OF TORTS, 2nd ed., §652C, comment a.
[28] Griswold v. Connecticut, 381 U.S. 479 (1965).
[29] Whalen v. Roe 429 U.S. 589 (1977). この事件は，乱用の危険のある特定の薬物を患者に調剤する際に，薬名，量，患者名，住所，年齢をニューヨーク州に報告させることとしたニューヨーク州法が患者のプライバシーの侵害にあたるかが争われ，結論としては，プライバシーの侵害はないとされた。

憲法上保護されるプライバシー領域（zone of privacy）は，「ある種の重要な決定をする際の独立性」（independence in making certain kinds of important decisions）と「私的事項の開示を避ける個人の利益」（individual interest in avoiding disclosure of personal matters） の 2 つの異なるタイプの利益に拡張されると判示した。後者は，ワーレン判決で初めて示されたものであり，ここに憲法上の情報プライバシー権（constitutional right to information privacy）が承認された[30)]。

４　公正な情報取扱原則の成立とプライバシー関連法の制定

1960 年代の情報化社会の進展に伴い，アラン・F・ウエスティン教授を始めとして，プライバシーを「自己に関する情報に対するコントロールの権利」として他人が自己に関する情報を利用できる程度を決定することができる積極的な権利として捉える見解が提唱された[31)]。1973 年，米国保健教育福祉省（U.S. Department of Health, Education, and Welfare）は，国内のデータ処理手続きに関し大規模な検討を行い，報告書を作成した（HEW Report）[32)]。同省は，この報告書において，公正な情報取扱原則（Code of Fair Information Practices, “FIPs”）が確立されるべきことを提言した。この公正な情報取扱原則（FIPs）は，自己に関する情報へのコントロールの手段を定め，現在のアメリカのプライバシー保護立法及び運用実務において重要な役割を果たしている。

具体的な FIPs の内容は，①存在自体が秘密になっている個人データ記録システムは存在してはならない。②個人が，自己に関するいかなる情報が記録中にあり，それがどのように利用されているかを知る方法がなければならない。③ある特定の目的のために取得された個人情報が，本人の同意なく，その他の目的のために利用されまたは利用可能な状態におかれることを，本人が防止する方法がなければならない。④本人が，自己を識別可能な情報の記録を訂正する方法がなければならない。⑤個人識別可能な個人データの記録を作成，維持，利用又は頒布する組織は，利用目的に従ってデータの信用性を確保し，データ

---

30) 同じ年の Nixon v. Administrator of General Services, 433 U.S. 425 (1977) 以降，憲法上の情報プライバシー権を述べた連邦最高裁判決はないが，連邦控訴審裁判所の多数は，多くの事件でプライバシー権を承認している。

31) Alan Westin, *Privacy and Freedom*, ATHNEUM NEW YORK, 1967.

32) U.S. Department of Health, Education and Welfare, “Records, Computers, and the Rights of Citizens: Report of the Secretary’s Advisory Committee on Automated Personal Data Systems”, 1973, at http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm (as of March 23, 2010).

の誤用を防止するための合理的な予防措置を取らなければならない，というものであった。

1970 年代の初めから，連邦議会は，様々な分野において，プライバシー保護に関する法律を制定した。1980 年には，公正な情報取扱原則（FIPs）を基礎とした経済開発協力機構（OECD）8 原則が発表され，立法に影響を与えた。1990 年代には，インターネットが普及しはじめたこと及び，個人情報を収集してそのデータベースをマーケティングに利用するデータベース産業が急成長してきたことから，これに対応した法律の制定も行われている。

表 3：FIPs に基づく現在の連邦政府における運用実務[33)]

最小限化	必要な情報のみ取得する。
通　知	情報取得時に，本人に対し，関係当局，取得目的，利用方法，他者に開示される可能性について通知する。
情報の質	正確で関連のある情報のみ，必要な限度で維持する。
アクセスと補正	法律に従い，本人に自己の情報の閲覧を認め，もし本人が誤っていると考える場合には補正手段を与える。
保　護	存続期間中，情報の保護を行う。

Ⅲ　アメリカにおけるプライバシー保護の個別立法例

１　アメリカにおけるプライバシー保護法制の概観

アメリカのプライバシー保護は，これまで見たように，徐々に形成されてきた憲法上，民事不法行為法上の保護を受ける他，数々の個別立法により保護される。公的部門においては，Privacy Act of 1974 を中心とした法律による規制が行われ，民間部門においては，自主規制を中心とし，特に必要性がある場合に

33) 2009 年 5 月に The American Society of Access Professionals（ASAP。Freedom of Information Act や Privacy Act に基づく情報開示請求に関与する政府職員や市民が設立した非営利団体）が主催した，主に政府職員向け研修会において国務省の担当者が配布したレジュメから翻訳して抜粋。

個別立法（連邦法及び州法）が行われている。ただし，民間部門における個別立法は多数ある。特に著名なものとして，金融情報分野での Fair Credit Reporting Act of 1970（FCRA）や医療情報分野での Health Insurance Portability and Accountability Act of 1996（HIPAA）がある。なお，盗聴行為等の規制に関する Electronic Communications Privacy Act of 1986（ECPA）のように公的部門及び民間部門双方に適用される条項を有する立法例も見られる。2001 年 9 月 11 日のアメリカ同時多発テロ後，USA PATRIOT ACT（愛国者法）が成立し，これまでのプライバシー保護立法の内容が大幅に緩和され，捜査機関は，個人情報データベース提供会社，信用報告機関，電話会社，インターネットプロバイダー，クレジットカード会社等の民間部門が保有する個人情報を容易に取得することができるようになった。盗聴や電子メール閲覧も秘密裏に容易になしうる。これにより，アメリカ連邦政府は，極めて広範な個人情報を取得することが可能となっている。

アメリカの民間事業者におけるプライバシー保護を考える上では，EU とアメリカとの間で締結されたセーフ・ハーバー協定[34]も重要である。1995 年に採択された EU 個人データ保護指令 25 条では，十分なレベルの個人情報保護措置を確保していない国には EU 加盟国の個人データの移転ができないことになったため，自主規制を中心とするアメリカのプライバシー保護法制に対し，EU から個人情報保護措置が不十分ではないかとの懸念が示された。これに対し，アメリカは，自主規制と個別立法の枠組みを維持しつつ，EU 個人データ保護指令に適合するため，「セーフ・ハーバー」という方法を提案した。これは，セーフ・ハーバー・プライバシー原則（告知，選択，第三者移転，アクセス，セキュリティ，データの完全性，実施といった項目からなる）を遵守し，アメリカ商務省に対し，同原則に従っているとの自己証明書を提出することで個人情報保護措置の十分性を満たすものと見なす制度である[35]。自主規制を中心とするが，違反を繰り返した場合は，連邦取引委員会（FTC）により罰金，違反行為の停止命令などの法的制裁が加えられる。2 年間の交渉を経てセーフ・ハーバー協定は 2000 年 7 月に発

---

34) 詳細は，石井・前掲注 1）449 頁以下参照。

35) セーフ・ハーバー協定については，EU がアメリカの脅しに屈して個人情報保護が不十分な現状に目をつぶったに過ぎず，十分に遵守されてないとの指摘もある。James B. Rule, *Privacy in peril*, Oxford University Press, 2007, p.138.

効した。同協定は，アメリカが自主規制と個別立法によるプライバシー保護の枠組みの維持をいかに強く望んでいるかということを示している[36]。

以上のとおり，アメリカにおけるプライバシー保護法制は複雑であり，これを一言でまとめることは困難である。プライバシー問題を専門とするアメリカ人であっても，個別の問題状況に応じて，必要な規制を連邦法及び州法を含めて調査することを要することが多いようである。アメリカのロースクールにおけるプライバシー法講義においては，1 つの法律を深く掘り下げるよりも，どのような分野にどのような法規制があるかを広く習得することが中心となる。以下では，プライバシー保護規定を持つ連邦法を広く紹介し，個別立法が全体としてどのような分野を保護しているのか見ていきたい[37]。

２　個別立法

(1) 政府保有情報分野

(a) Freedom of Information Act of 1966（FOIA）

日本の情報公開法に相当する。同法は，連邦政府の行政機関を対象に，その保有する記録を原則として開示することを定めたものである。ただし，プライバシーに該当する情報は，開示が禁止される。個人識別情報を広く対象としていると解されているが，最終的に開示が禁止される例外条項に該当するか否かは，プライバシーの利益と開示による公益の比較衡量により決せられる[38]。

(b) Privacy Act of 1974（PA）[39]

政府の個人情報保有の必要性と個人のプライバシーの保護を調整する目的で，公正な情報取扱原則（FIPs）を具体化した法律である。日本の「行政機関の保有する個人情報の保護に関する法律」（以下「行政機関個人情報保護法」という）に相当する。

---

[36] 日本では，EU からのプライバシー保護が不十分であるとの指摘を受けて，これを一つの契機として個人情報保護法が制定された。

[37] いくつかの重要な立法例については，より詳細な解説がある日本の文献を注に掲示したので参考にしていただきたい。また，アメリカの立法例を広く紹介した日本の文献として，石井・前掲注 1）419 頁以下，及び榎原猛編『プライバシー権の総合的研究』251 頁以下〔岡田安巧〕（法律文化社，1991 年）。

[38] 宇賀克也『情報公開法　アメリカの制度と運用』264-280，294-296 頁（日本評論社，2004 年）。

[39] 詳細に論じた日本の文献として，阪本・前掲注 1）249 頁以下及び 264 頁以下，並びに石井・前掲注 1）420 頁以下，榎原・前掲注 37）251 頁以下参照。

連邦政府の行政機関[40]が保有する記録システムに含まれる個人を識別可能な記録についてその開示を制限し，本人に当該記録へのアクセス及びこれを修正する権利を認めている[41]。また，対象機関は，記録システムの名前，所在，目的，内容等について公表しなければならず（System of Records Notice, “SORN”），これらの記録の安全性及び秘密性を確実にするため，適切な組織的，技術的及び物理的防止策を講じなければならない。

対象機関が同法の定めに違反した場合には，当該個人は，連邦裁判所に民事訴訟を提起でき，裁判所は，当該機関が記録にアクセスすることを禁止することができる。また，裁判所が当該機関の行動を故意による（intentional or willful）と認めた場合には，当該個人は，現実の損害（ただし，法文上，いかなる事件においても賠償を受ける資格を有する者は 1000 ドル以上の金額を受けるとされ，法定最低賠償額が定められている[42]）及び訴訟費用（合理的な弁護士費用を含む）の賠償を受けることができる。さらに，違法な個人情報の開示には，刑事罰もある。

(c) Driver’s Privacy Protection Act of 1994（DPPA）

同法は，各州の自動車局（Department of Motor Vehicle, “DMV”）が自動車記録の関係で取得した個人情報の開示を制限する[43]。

同法制定以前，多くの州は，自動車記録（名前，住所，電話番号，社会保障番号，医療情報，身長，体重，性別，目の色，顔写真，生年月日等を含む）を民間に販売していた[44]。同法は，このような慣行を停止するため制定された。

(d) E-Government Act of 2002

同法は，電子政府推進のために定められた。この中で，連邦政府の機関が新たな電子的情報収集又は IT システムを導入する場合や，新たなプライバシーリスクを作り出すシステム変更を行う場合には，プライバシー影響評価（Privacy impact assessment, “PIA”）を行うことを要求している。

---

40) 州および地方の機関，私的組織は対象外である。
41) アクセス及び修正について，訴訟で争うことも可能である。
42) 連邦最高裁は，Doe v. Chao, 540 U.S. 614 (2004) において，原告が法定最低金額の賠償を受けるために，何らかの現実の損害を立証する必要があるとの立場をとった。
43) 連邦による州への規制となるため，サウス・カロライナ州は，連邦主義制度の原則に違反しているとして提訴したが，連邦最高裁は合憲性を認めた（Reno v. Condon, 528 U.S. 141 (2000)）。
44) 前記 Reno v. Condon 事件判決中に，ウィスコンシン州では，その販売で毎年 800 万ドルの収入があったことが記されている。

(2) 捜査分野

(e) Privacy Protection Act of 1980（PPA）

同法は，新聞，本，放送等での報道目的で所持する資料の捜索差押については，裁判所で異議申し立てをすることが認められる召喚令状を要求するものである。

同法は，連邦最高裁が，事件と無関係の学生新聞が当該事件を報道したところその取材資料が捜索差押令状に基づき捜査機関の捜索差押を受けた事件で，広く新聞社に対する捜索差押を認める判決をしたこと[45]に対応するため立法された。

(f) Electronic Communications Privacy Act of 1986（ECPA）

同法は，従来の電話盗聴法（Title III of the Omnibus Crime and Control Act of 1968）を新たなコミュニケーション手段の発達に合わせて拡張したものである。大きく分けて 3 つのパートからなり，第 1 編は，人のコミュニケーション（電線経由，口頭，電子的手段による）の傍受の規制（Title I 通称“Wiretap Act”）。第 2 編は，蓄積されたコミュニケーション及びインターネットサービスプロバイダーのようなコミュニケーションサービス提供者の保有する記録へのアクセス規制（Title II 通称“Stored Communication Act”）。第 3 編は，通話番号記録器等の通話者を特定する機器の規制（Title III 通称“Pen Register Act”）である。規制対象行為を行うには裁判所の命令（Court Order）が必要であり，行為の性質に応じて裁判所の命令を得るための要件が細かく規定されている。これらの条項の大部分は，政府だけでなく，民間にも適用がある。特に雇用関係において，雇用者が被用者に対して調査を行う際に問題となることが多い[46]。違反に対しては，行為の性質に応じて損害賠償義務及び禁固刑・罰金刑が定められている。また，第 1 編の電線経由，口頭によるコミュニケーションに関する規制違反で取得された証拠は，証拠排除法則が適用される。

---

[45] Zurcher v. Stanford Daily, 436 U.S. 547 (1978).
[46] Daniel J. Solove &Paul M. Schwartz, *supra* note 4), p.296.

(3) 金融・商取引分野

(g) Fair Credit Reporting Act of 1970（FCRA）[47)]

アメリカでは，1960 年代までに，債権者が債務者の返済能力を確認する手段として，信用報告機関（credit reporting agencies）の報告書を利用することが普及してきた[48)]。この信用報告書（Credit report）には，個人の詳細な借入履歴，金融口座情報，主要な負債，破産履歴，担保権情報等が記載されている。信用報告書の影響力が高まるにつれて，その信用報告書の不正確さとこれに対する信用報告機関の責任の欠如が問題とされるようになり，連邦議会は同法を制定した。

同法は，信用情報の利用を，裁判，与信，雇用，保険，不動産賃貸等に限定する。そして，本人に信用報告機関の保有する自己の記録へアクセスすることを可能とし，本人は，不正確な情報について争うことができる。同法は，信用報告機関に，可能限り正確な情報を確保する合理的手続を取る義務を課しつつ，債権者と信用報告機関について，消費者に対する悪意によって情報が記録に保有されたのでない限り，名誉毀損，プライバシー侵害等の訴訟から免責している。

同法の規定に故意に違反した者は，消費者に対し，100 ドルから 1000 ドルの間で現実の損害の賠償義務を負う他，懲罰賠償及び弁護士費用その他の訴訟費用も賠償する義務を負う。過失により違反した者は，現実の損害賠償と弁護士費用その他の訴訟費用を賠償する義務を負う。同法に基づく責任追及は，原則として責任発生時から 2 年以内に行わなければならない。

(h) Right to Financial Privacy Act of 1978（RFPA）

同法は，銀行その他の金融機関が個人の金融情報を，召喚令状（subpoena）又は捜索令状（search warrant）等なくして連邦政府に開示することを制限する。

同法は，連邦最高裁が，第三者の保有する個人の情報を連邦政府が取得することについては合衆国憲法修正 4 条（令状主義）の適用がないとの立場（Third party doctrine）をとり，銀行の顧客の金融情報を政府が取得することについて，顧客は

---

47) 詳細に論じた日本の文献として，阪本・前掲注 1）287 頁以下参照。

48) その背景には，アメリカ人の行動範囲の増大と小売業界の統合により，地元の限られた店での商取引が減少し，個人の信用を把握することが困難になってきたことがあげられる。James B. Rule, *supra* note 35), p.100.

同条の保護を受けないと判断したことから[49]，顧客の金融情報についてプライバシーを保護するために立法された。

(i) Cable Communications Policy Act of 1984（CCPA）

同法は，ケーブル通信サービスの利用者の記録を保護するために定められた。サービス提供者は，個人情報の収集と利用の内容について利用者に通知しなければならず，利用者は，自己の情報にアクセスすることができる。また，サービス提供に不可欠でない個人情報を収集する場合には，あらかじめ本人の同意を得る必要がある。サービス提供者は，原則として，個人情報を同意なく開示してはならない。例外的に，合法な商業活動又は裁判所の命令を求めるときには同意なく個人情報を開示することが可能であるが，サービス提供者は，利用者に対し開示先を明らかにしなければならず，また利用者の視聴内容については明らかにしてはいけない。同法の違反に対しては，民事訴訟を提起し，現実の損害（法定最低限度額として 1000 ドルまたは違反 1 日あたり 100 ドルの高い方），懲罰賠償及び弁護士費用の賠償を受けることができる[50]。

(j) Video Privacy Protection Act of 1988（VPPA）

同法は，ビデオサービスの提供者について，利用者が利用したビデオのタイトルを本人の同意なく開示することを原則として禁止している。また，定期的に不要となった個人情報を抹消することを求めている。

同法は，連邦最高裁判事候補者の利用していたビデオ店から，報道関係者が同候補者のビデオ視聴履歴を取得したことをきっかけに制定された。同法の違反に対しては，現実の損害（法定最低限度額 2500 ドル），懲罰賠償，弁護士費用の賠償及び差止めが認められる。同法に基づく責任追及は，違反行為の日又は違反発見の日から 2 年以内に提訴しなければならない。さらに，同法に違反して取得された証拠には，証拠排除法則が適用される[51]。

(k) Telephone Consumer Protection Act of 1991（TCPA）

同法は，個人が電話セールス業者に再び電話をかけないことを要求することを認める。電話セールス業者が電話をやめない場合，当該個人は，当該電話セールス業者に対して，それぞれの電話ごとに，少額訴訟による損害賠償請求（実

[49] United States v. Miller, 425 U.S. 435 (1976).
[50] Daniel J. Solove &Paul M. Schwartz, *supra* note 4), pp.800-801.
[51] *Id*., pp.794-795.

損害か 500 ドルの大きい方）をすることができる。ファクシミリへの送信も同様に規制される。2003 年に，連邦通信委員会（FCC）は，同法の授権に基づき，連邦取引委員会（FTC）と合同で，全国電話拒絶名簿（national “Do Not Call” list）[52]を創設した[53]。同名簿に登録した場合，当該個人に対する電話セールスについて同法の適用がある。

(l) Identity Theft and Assumption Deterrence Act of 1998

同法は，なりすまし犯罪（Identity Theft）[54]の増加を受けて，違法な行為に利用するため正当な権限なく他人の本人確認手段（mean of identification）を譲渡，利用することを犯罪としている。

(m) Children’s Online Privacy Protection Act of 1998（COPPA）

同法は，12 歳以下の子供の情報をインターネットのウエブサイトで収集及び利用することを制限する。子供向けサイトの運営者（子供向けサイトでなくとも，子供から個人情報を収集していることを認識している運営者を含む）は，どのような情報が収集され運営者がこれらの情報をどのように利用するか等を記載したプライバシーポリシーを掲示しなければならない。そして，子供から個人情報を収集し，利用等することについて，親の同意を得なければならない。同法の違反に対しては，連邦取引委員会法（Federal Trade Commission Act）における「不公正または詐欺的な取引」として，連邦取引委員会（FTC）が権限を行使し，罰金を科すことができる[55]。個人からの民事訴訟はできず，州が市民の利益のため，差止と損害賠償を求めて民事訴訟を提起することが認められている。

---

[52] 全国電話拒絶名簿への登録は，以下の Web サイトで可能である。<https://www.donotcall.gov/>（2010 年 3 月 23 日最終アクセス）。電話番号と電子メールアドレスだけを記入し（氏名，住所は記入する必要がない。），送られてきた電子メールのリンク先をクリックすれば登録が完了するという極めて簡便なものである。

[53] Paul M. Schwartz & Daniel J. Solove, *INFORMATION PRIVACY STATUTES AND REGULATIONS 2008-2009*, ASPEN PUBLISHERS, 2008, p.493.

[54] 典型的には，他人の個人情報を利用して，他人になりすまして，同人名義のクレジットカードを作成して買い物をしたり，同人の既存口座から現金を引き出したりする行為である。当該犯罪は，被害者の信用情報を著しく低下させ，その回復には相当の時間と労力を要する。

[55] 連邦取引委員会（FTC）は，もともと独占取引等を監視する組織であって，プライバシー保護を目的とした組織ではなかったが，1998 年から，連邦取引委員会法に基づき，COPPA の適用外でも，一定の産業分野でプライバシーポリシーに反する取引実態がある場合には，「不公正または詐欺的な取引」として，その権限を行使し，罰金を科すようになった。多くの事案は，和解で終了するが，その和解内容は，具体的なプライバシーポリシーの記載の仕方を示すなど，アメリカの経済分野におけるプライバシールールを多く生み出しており，プライバシー保護の実務上重要な役割を演じている。Daniel J. Solove & Paul M. Schwartz, *supra* note 4), pp.776-787.

(n) CAN-SPAM Act of 2003

正式名称は，Controlling the Assault of Non-Solicited Pornography and Marketing Act である。同法は，いわゆるスパムメールを規制するものであり，主要目的が広告または宣伝である商業的電子メールに適用される。違反行為に対しては，民事上また刑事上の責任追及が可能である。

(o) Fair and Accurate Credit Transactions Act of 2003（FACTA）

同法は，Fair Credit Reporting Act（FCRA）を修正するもので，なりすまし犯罪（Identity Theft）に対する保護を与える。同法は，信用報告機関に，毎年無料で信用報告書を提供するように求めている[56]。また，多くの信用報告機関が本人に明らかにしてこなかったクレジットスコア（3 桁の点数で個人の信用度を評価したもの）を本人に明かにするよう求めている。さらに，詐欺の被害者が，信用報告機関 1 社に対し，その事実を報告すれば，同機関は，他の信用報告機関にもこれを通知しなければならない。また，一定の条件の下，なりすまし犯罪の被害者は，犯人に利用された債権者（クレジット会社等）に対し，被害者の名前で行われた詐欺的取引の詳細を提供するように求める権利を有する。

(4) 医療分野

(p) Health Insurance Portability and Accountability Act of 1996（HIPAA）[57]

同法は，従業員が仕事を変えた時に従前の健康保険の状態をそのまま引き継げるようにすることを主な目的としている。これに伴い，特に個人の医療情報が共有，移転されるため，連邦議会はその保護を検討した。連邦議会は，同法内にプライバシー保護の規定を設けず，医療情報のプライバシーに関し，新たな包括的な立法をするつもりであったが，期限までに立法することができず，結局，HIPAA の条項に基づき，保健福祉省（Department of Health and Human Services（HHS））が必要な連邦規則の制定に着手し，プライバシー規則の最終版が 2000 年 12 月に出された（45 C.F.R. parts 160 through 164）[58]。

同法の適用対象は，①医療保険者（保険会社等），②医療情報処理者（標準化されていない医療情報を受け取り標準化されたフォームに加工する者等），③医療サービス

---

[56] 以下の HP から，信用報告機関大手 3 社の信用報告書の入手が可能である（なお，同 HP はアメリカ国内のプロバイダーからしかアクセスできない）。<https://www.annualcreditreport.com/cra/index.jsp>（2010 年 3 月 23 日最終アクセス）。

[57] 日本の文献としては，石井・前掲注 1）446 頁以下参照。

[58] Daniel J. Solove & Paul M. Schwartz, *supra* note 4), pp.431-432.

提供者（医者，病院，薬剤師等）で同法の取引規則に定められた請求等の一定の取引に関し，一定の標準化された電子的フォームで医療情報を処理・送信する者（第三者に委託する場合も含む），に限られる[59]（以下，HIPAA 対象者という）。このため，それ以外の個人の健康情報を取り扱うウエブサイトなどは対象にならない。

保護の対象となる情報は，HIPAA 対象者及びその業務委託者が保有または送信した個人識別可能な医療情報（電子的か紙か口頭かといった形態を問わない）である（以下，対象情報という）[60]。

HIPAA 対象者及び業務委託者が対象情報を利用，開示するには，原則として書面による本人の承諾が必要である。例外として，①本人に開示する場合，②HIPAA 対象者が行う治療行為，支払関係行為，医療関係行為（医療サービスの評価及び改善のための行為，医療サービス提供者・保険サービスの評価・信任・認定などの行為，法令順守プログラムにおける医学的再検討・監査・法的サービス，保険のリスク評価，経営計画策定・管理，対象情報を個人識別できない形に加工する行為等）に対象情報を利用する場合，③一定の状況下で本人に同意不同意の選択の機会を与えた場合（本人が選択できない緊急時は，本人にとって最も利益となる利用・開示ができる），④公益目的及び慈善行為（法律の求めによる場合，公衆衛生活動，司法・行政手続に利用する場合，献体・献眼，研究目的，人の健康安全に対する重大な危険がある場合，重要な政府機能に必要な場合等），⑤偶発的な利用・開示（ただし，プライバシー規則の求めに応じた相当な保護策を講じ，当該情報が最小限に限定された場合のみ），⑥限定的なデータ（対象情報から本人，親族，同居人，雇用主の識別名を取り除いたもの）を受領者が同データにつき特定の保護策を講じることに同意して研究，医療関係行為，公衆衛生目的で利用する場合には本人の書面による承諾は必要ではない[61]。これらの例外に該当するか否かは，HIPAA 対象者が自身の職業倫理と最善と信じる判断に基づいて判断する[62]。さらに，対象情報を利用・開示する場合，原則として，HIPAA 対象者は対象情

---

[59] U.S. Department of Health & Human Services, “Summary of the HIPAA Privacy Rule”, 2003, pp.2-3, at http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf (as of March 23, 2010).
[60] *Id*., p.2.
[61] *Id*., pp.4-9.
[62] *Id*., p.5.

報について最小限必要な範囲にとどめるよう合理的な努力をしなければならない[63]。

本人は，HIPAA 対象者に対して，自己の対象情報にアクセスし，自己の対象情報を修正し，開示先の報告を求め，また，対象情報の利用・開示にあたり，その情報の範囲を一定範囲に制限することを求める権利を有する（制限の求めに応じる義務はないが，合意をした場合は守らなくてはならない）[64]。

HIPAA 対象者は，プライバシー規則に従ったプライバシーポリシーと手続を定め，プライバシー担当者を指定しなければならない。また，従業員らが適切に行動できるように訓練，監督しなければならない。さらに，プライバシー規則に反する対象情報の利用・開示を防止するための組織的・技術的・物理的保護策を講じなければならない。そして，HIPAA 対象者は，対象情報の利用・開示の方法，HIPAA 対象者のプライバシー保護義務，プライバシー実務，本人が保健福祉省に対して自己のプライバシー権の侵害について申し立てる権利，プライバシー担当者の連絡先等について通知しなくてはならない[65]。

同規則に違反して開示した場合には，刑事罰と年間最高 2 万 5000 ドルまでの民事損害賠償請求を受ける。特定の違法な開示には，最長 10 年の禁固と最高 25 万ドルの民事賠償請求が認められる。ただし，個人は民事訴訟を提起できず，保健福祉省が行う。

(5) その他

(q) Family Educational Rights and Privacy Act of 1974（FERPA）

同法は，原則として学校が生徒もしくは親の同意なく，その教育記録を開示することを禁止する。学校は，請求により，生徒もしくは親に教育記録を閲覧させなければならない。また，学校は，教育記録に誤りがないことおよびプライバシーその他の権利侵害がないことを確実にするため，生徒にその内容について争うための聴聞の機会を与えなくてはならない。同法の違反に対しては，個人の学校に対する不服申し立ての後，教育省が調査をして，必要な指導を行う。

---

63) *Id*., p.10.
64) *Id*., pp.12-13.
65) *Id*., p.11, p.14.

(r) Employee Polygraph Protection Act of 1988

同法は，民間の雇用者が被用者に対してポリグラフ検査をすることを原則として禁じている。雇用者は，例外的に，係属中の窃盗，横領等の自己のビジネスにおける経済的損害の捜査に関連して，合理的に関与が疑われる雇用者に対してポリグラフ検査を行うことはできる。同法の違反に対しては，最高 1 万ドルまでの民事罰が科される。労働長官は，提訴して裁判所の禁止命令等を得ることができる。また，違反した雇用者は被用者に対して，復職，昇進，逸失給与等の手当をする責任を負う。

Ⅳ　アメリカにおけるプライバシー保護の課題と日本への示唆

1　日本のプライバシー保護状況の概観[66)]

日本では，アメリカのプライバシーに関する議論を参照しながらプライバシー保護が図られてきた。

不法行為法によるプライバシー保護としては，1964 年，モデル小説に関する『宴のあと』事件判決（東京地判昭和 39 年 9 月 28 日判時 385 号 12 頁）が，私生活をみだりに公開されないことについてプライバシーの権利侵害による不法行為の成立を認めたのが先例とされている。その後，最高裁平成 15 年 3 月 14 日判決（民集 57 巻 3 号 229 頁）は，ノンフィクション『逆転』事件の最高裁平成 6 年 2 月 8 日判決（民集 48 巻 2 号 149 頁）を引用し，「プライバシーの侵害については，その事実を公表されない法的利益とこれを公表する理由とを比較衡量し，前者が後者に優越する場合に不法行為が成立する」と判示し，また，早稲田大学江沢民事件判決（最判平成 15 年 9 月 12 日民集 57 巻 8 号 973 頁）において，「個人情報についても，本人が，自己が欲しない他者にはみだりにこれを開示されたくないと考えることは自然なことであり，そのことへの期待は保護されるべきものであるから，本件個人情報は，上告人らのプライバシーに係る情報として法的保護の対象となるというべきである。」「上告人らに無断で本件個人情報を警察に開示した同大学の行為は，上告人らが任意に提供したプライバシーに係る

66) 堀部・前掲注 1）43 頁以下及び，三宅弘=小町谷育子『個人情報保護法　逐条分析と展望』58 頁以下（青林書院，2003 年）。

情報の適切な管理についての合理的な期待を裏切るものであり，上告人らのプライバシーを侵害するものとして不法行為を構成するというべきである。」と判示している。このように我が国の法制度上プライバシー侵害に対して不法行為法による保護が与えられていることは明かである。

憲法による保護として，最高裁は公道での警察官が犯罪捜査のために行った写真撮影の適法性が問題となった京都府学連事件判決（最判昭和 44 年 12 月 24 日刑集 23 巻 12 号 1625 頁）において，「個人の私生活上の自由の一つとして，何人も，その承諾なしに，みだりにその容ぼう・姿態（以下「容ぼう等」という。）を撮影されない自由を有するものというべきである。これを肖像権と称するかどうかは別として，少なくとも，警察官が，正当な理由もないのに，個人の容ぼう等を撮影することは，憲法一三条の趣旨に反し，許されないものといわなければならない。」と判示し，また指紋押なつ拒否事件判決（最判平成 7 年 12 月 15 日刑集 49 巻 10 号 842 頁）において，「指紋は，指先の紋様であり，それ自体では個人の私生活や人格，思想，信条，良心等個人の内心に関する情報となるものではないが，性質上万人不同性，終生不変性をもつので，採取された指紋の利用方法次第では個人の私生活あるいはプライバシーが侵害される危険性がある。このような意味で，指紋の押なつ制度は，国民の私生活上の自由と密接な関連をもつものと考えられる。憲法一三条は，国民の私生活上の自由が国家権力の行使に対して保護されるべきことを規定していると解されるので，個人の私生活上の自由の一つとして，何人もみだりに指紋の押なつを強制されない自由を有するものというべきであり，国家機関が正当な理由もなく指紋の押なつを強制することは，同条の趣旨に反して許されず」と判示している。このことから，最高裁は，憲法 13 条に基づきプライバシーについて一定の保護を与える趣旨と解される。

個人情報保護に関する動きとして，情報化社会の進展に伴い，政府は 1970 年に行政事務処理用統一個人コードの検討を始めたが，「国民総背番号制」との国民の強い批判にさらされて，立ち消えとなった。同年には，佐藤幸治教授が「プライヴァシーの権利（その公法的側面）の憲法的考察（一）（二）」との論文

において自己情報コントロール権を提唱している[67]。1980 年には経済協力開発機構（OECD）の「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」が採択され，いわゆる OECD8 原則[68]を踏まえた国内法の制定が求められたことを受けて加盟国である日本においてもプライバシー保護立法についての議論が高まった。前科照会事件最高裁判決（昭和 56 年 4 月 14 日民集 35 巻 3 号 620 頁）で伊藤正己補足意見は「国又は地方公共団体においては，行政上の要請など公益上の必要性から個人の情報を収集保管することがますます増大しているのであるが，それと同時に，収集された情報がみだりに公開されてプライバシーが侵害されたりすることのないように情報の管理を厳にする必要も高まつているといつてよい。」と述べ，個人情報保護の重要性を指摘している。1984 年には福岡県春日市で個人情報保護条例が制定されるなど地方レベルで個人情報保護条例の制定が始まり，国レベルでも 1988 年に「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」（旧行政機関個人情報保護法）が制定された。通商産業省は，1997 年，「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」（告示第 98 号）を告示している。1999 年の住民基本台帳法の改正により，2002 年以降住民基本台帳ネットワークシステムが導入され，国民それぞれを異なった数字で把握する住民票コード及び身分証明証となる住民基本化台帳カードが制度化されたが，これに対してプライバシー侵害だとする反対運動は盛り上がりを見せた。そして，EU 個人データ保護指令への対応や住民基本台帳ネットワークシステム導入を契機として，2003 年，個人情報保護法，行政機関個人情報保護法及び独立行政法人等個人情報保護法が成立した。個人情報保護法は，民間部門について一般的に適用される具体的規定を持っているだけでなく，国の責務及び地方公共団体の責務も定めていることから，公的部門に関する行政機関個人情報保護法，独立行政法人等個人情報保護法及び個人情報保護条例に対して基本法的な性格を有している点で特殊である。また，民間部門については一般法である個人情

---

67) 佐藤幸治「プライヴァシーの権利（その公法的側面）の憲法的考察（一）」法学論叢（京都大学）86 巻 5 号 1-53 頁（1970 年），「プライヴァシーの権利（その公法的側面）の憲法的考察（二）」法律論叢（京都大学）87 巻 6 号 1-40 頁（1970 年）。

68) OECD8 原則は，現在の日本の個人情報保護法に強い影響を与えているプライバシー保護の原則であり，①収集制限の原則，②データ内容の原則，③目的明確化の原則，④利用制限の原則，⑤安全保護の原則，⑥公開の原則，⑦個人参加の原則及び⑧責任の原則からなる。

報保護法に加えて，同法に基づいて医療や金融など 24 分野について 37 のガイドラインが策定されている（2008 年 4 月 1 日現在政府発表）。

このように，日本においては，アメリカで始まったプライバシーの議論を参照しつつも，現在は民間部門においても一般法を持つに至っており，その法制度は異なるものとなっている。

２　アメリカの法制度の日本への示唆

(1) 個別立法の問題点

プライバシー問題は時代の変化と共に新たな保護対象（保護分野）を生ずるが，アメリカの個別立法では，このような時代の変化に対して立法が追いつかないことが多く見られる。例えば Driver’s Privacy Protection Act of 1994（DPPA），Right to Financial Privacy Act of 1978（RFPA）及び Video Privacy Protection Act of 1988（VPPA）などがその例である。これらの立法例は，社会的にプライバシー問題が生じた後に，その対策として遅ればせながら成立したものである。これに対して，日本の個人情報保護法のように，包括的立法により，例えば第三者提供や目的外利用を一般的に制限しておけば，ある程度時代が変化して新たな保護対象ができたとしても一定限度のプライバシー保護は可能であると考えられるから，包括的立法と比較して個別立法は，立法がない分野のプライバシー保護が弱くなりやすいという問題を有すると言える。この点，新たな保護対象については後追いでも速やかに立法をしていけば個別立法でもプライバシー保護を十分になしうるという考えもありうる。しかし，立法されるまでの間に個人情報の商業利用（例えば後述のプロファイリングビジネス）が既得権として確立してしまうと，当該分野の法的規制には業界からの激しい抵抗（ロビー活動）があり，十分なプライバシー保護は困難であることが多い。阪本昌成教授は，「アメリカのプライヴァシー保護の動向は，その基本的精神，それをうけた法案，そしてその審議段階での討論においては，われわれが学ぶべきものを豊富にもちあわせている。しかしながら，最終的にできあがった法律は，さまざまな妥協の産物以外の何物でもなく，ザル法的性格を色濃くしてしまっている。われわれが，アメリカの体験・法律から学ぶべきものがあるとすれば，その長所よりも

短所からであろう。」と述べている[69]。このように個別立法は社会の変化に対応して十分なプライバシー保護を行うことが困難という問題を有する。以下では，それにより引き起こされた社会的問題を紹介する。

アメリカ社会において個人情報の高度の商業的利用のプライバシーに対する危険性が認識され，その規制が行われたのは，1970 年の Fair Credit Reporting Act（FCRA）制定時である。同法は，信用報告機関が作成した個人の金融情報等に関する報告書の利用（売買）を規制した。しかし，同法は，既成事実の追認をしたに過ぎないと指摘されている[70]。その後も個人情報を大量に収集して商業的利用をすることはやむことがなかった。例えば Cable Communications Policy Act of 1984（CCPA）は，ケーブル通信サービス業者（ケーブルテレビ局）が利用者の視聴記録等を無断で売買することを規制しようとしたものである。また，Driver's Privacy Protection Act of 1994（DPPA）は，多くの州が，自動車記録（名前，住所，電話番号，社会保障番号，医療情報，身長，体重，性別，目の色，顔写真，生年月日等を含む）を民間に販売している慣行を停止するため制定された。

上記の立法例からわかるのは，アメリカにおいていかに多くの種類の個人情報が大量に売買されているかという実態である。コンピューター処理技術の発達に伴い，大量の個人情報を 1 つに集積・統合し，データの中に隠れているそれぞれの項目間の相関関係を洗い出してこれを意味づけることが可能となった。わかりやすい例で言えば，特定の薬を購入した者が，特定の病気にかかっているという事実を探り出すことである。また，例えば特定の雑誌を購読する者は，特定のブランド品を好むことが多いとか，特定のブランド品を好む者は特定の信仰を持っているとか同性愛者が多いという事実であることもありうる。このように大量の個人情報のデータをコンピューターで処理して，あらゆる角度から個人の趣味嗜好や生活状況を分析し，特定の物品，サービスに興味関心を示すであろう者のリストを作成して販売し，購入者はこれを広告等に利用するのである。

---

[69] 阪本・前掲注 1）261 頁。

[70] James B. Rule, *supra* note 35), p.100. また，阪本・前掲注 1）287 頁には「特にアメリカの FCRA の立法目的は，コモン・ロー上消費者信用情報機関に認められてきた条件的免責特権を限定化する目的にでたものであり，消費者保護の観点からすれば，さほどドラスティックな立法ではない。我が国の立法化にあたっては，政治的妥協の産物である FCRA のもつ基本的脆弱さを他山の石としつつ比較対照されなければならない。」と述べられている。

アメリカでは，さらに収集分析された個人情報が個人の経済力評価に利用されている。すなわち，アメリカの大手信用報告機関（Equifax, Experian, Trans Union）は，ほとんど全てのアメリカ市民の詳細なクレジットの支払履歴，借入履歴，金融口座情報，主要な負債，破産履歴，担保権情報等の情報を収集，蓄積し，これに基づいて個人の信用力をクレジットスコアとして決定している。このスコアは，与信（貸金），雇用，保険，不動産賃貸といった日常生活の重要な取引において，その人物の経済的信用性を示すものとして頻繁に利用される。クレジットスコアが悪い場合には，普通の人より金利が高くなるといった不利な契約条件となったり，取引ができなくなったりするなど市民生活に重大な不利益が生ずる。保険会社は，個人データの相関関係の洗い出しにより，クレジットスコアが悪い人の保険金請求の確率が高いことを発見し，このスコアが悪い人に対しては保険料を上げているという事実も報告されている[71)]。

クレジットスコアは，クレジットカードの支払を怠った場合などに悪くなることから，まじめに支払っている人は良いスコアを得られ，不払いを繰り返す人より有利な取引条件になることは歓迎すべきだという人もいると思われる。しかし，うっかり支払を怠ったまま住所を変えてしまうと，不払いであることの連絡も届かないままスコアは低下し続ける危険がある。2003 年に Fair and Accurate Credit Transactions Act（FACTA）が制定されるまでは，クレジットスコアを本人が確認することは困難であったから，自身が知らない間にスコアが急降下し，住宅ローンの申込みを断られて初めて気づくという事態もあり得た。また，ほとんどのアメリカ市民のデータを大量に保有しているため，他人のデータと混同されるなどの誤りが生じることも珍しくなく，その訂正には非常に時間がかかるという問題もある。誤ってスコアが低下してから回復するまでには相当な時間がかかり，その間の社会生活は極めて不自由なものとなる。

さらに事態を悪化させるのは，なりすまし犯罪（Identity Theft）である。なりすまし犯罪とは，典型的には，他人の個人情報を利用して，他人になりすまして，同人名義のクレジットカードを作成して買い物をしたり，同人の既存口座から現金を引き出したりする行為である。アメリカでは，このなりすまし犯罪が大きな社会問題となっている。なりすまし犯罪は，被害者のクレジットスコアを

71) James B. Rule, *supra* note 35), p.109.

著しく低下させ，その回復には相当の時間と労力を要する[72]（ある調査では，被害回復には平均2年，消費時間は平均175時間との報告もある[73]）。信用情報回復までの間，被害者の就職活動やローンの設定等は容易でなく，現実の被害額よりも問題は深刻である[74]。問題の広がりをうけて，1998年にIdentity Theft and Assumption Deterrence Actが立法されたが，いまだに大きな社会問題であり，テロリストの資金源となっているとの指摘もある[75]。

このように，アメリカでは，個人情報の高度の商業的利用が進んでおり，そのことが市民生活に重大な影響を与えている。クレジットスコア制度は，個人の信用力を評価する便利なツールであるが，結果的にこれにより利益を受けるのは消費者ではなく企業側であり，クレジットスコアが正確に本人の信用力を評価しなくなった場合のリスクも全て消費者側に転嫁されてしまっており，プライバシーの観点からも消費者保護の観点からも非常に問題のある制度である。

日本では，1983年の貸金業の規制等に関する法律30条2項において信用情報の目的外利用の禁止が定められた（現在は貸金業法41条の38に同趣旨の規定が置かれている）。また，1984年には，割賦販売法に「信用情報を購入者の支払能力の調査以外の目的のために使用してはならない」との規定が追加された（現行法39条1項）。そして，2003年，個人情報保護法においては，利用目的の特定（15条），利用目的による制限（16条），取得に際しての利用目的の通知等（18条），第三者提供の制限（23条）等が定められたから，アメリカのように広く個人信用情報が利用される状況に直ちになることはないと考えられる。しかし，2006年の貸金業法の改正で指定信用情報機関制度が導入され，過剰与信防止のため指定信用情報機関同士の情報交流が義務づけられた（法41条の24第1項）。また，全国賃貸保証業協会は，2010年2月から家賃滞納歴などの賃貸信用情報をデータベース化するとしている[76]。このように各種信用情報が収集蓄積されやすい状況になってきていることから，これがアメリカのクレジットスコア制度のような

---

72) 特定の被害者の状況をレポートしたものとしてロバート・オハロー（中谷和男訳）『プロファイリング・ビジネス』103頁以下（日経BP社，2005年）。

73) Janine Benner, Beth Givens & Ed Mierzwinski, “Nowhere to Turn: Victims Speak Out on Identity Theft”, 2000, pt. II §1, §4, at http://www.privacyrights.org/ar/idtheft2000.htm (as of March 23, 2010).

74) Daniel J. Solove, *Understanding Privacy*, HARVARD UNIVERSITY PRESS, 2008, pp.126-127.

75) ロバート・オハロー・前掲注72）125頁。

76) 朝日新聞2009年9月30日朝刊。

個人信用情報の高度な商業的利用につながらないように適切に規制していく必要がある。

(2) 個人情報産業と政府の複合体が生み出す新たな脅威

Right to Financial Privacy Act of 1978（RFPA）は，銀行その他の金融機関が個人の金融情報を召喚令状（subpoena）又は捜索令状（search warrant）なくしてアメリカ連邦政府に開示することを制限する。また，Privacy Protection Act of 1980（PPA）は，新聞，本，放送等での報道目的で所持する資料の捜索差押については，裁判所で異議申し立てをすることが認められる召喚令状を要求するものである。これらの法律は，プライバシー関連法の中で比較的古い立法であるが，政府が民間の蓄積した情報を取得することの危険性を示している。

しかし，2001 年 9 月 11 日のアメリカ同時多発テロ後，USA PATRIOT ACT（愛国者法）が成立し，これまでのプライバシー保護立法の内容が大幅に緩和され，捜査機関は，個人情報データベース提供会社，信用報告機関，電話会社，インターネットプロバイダー，クレジットカード会社等の民間部門が保有する個人情報を容易に取得することができるようになった。盗聴や電子メール閲覧も秘密裏に容易になしうる。これにより，アメリカ連邦政府は，極めて広範な個人情報を取得することが可能となった。

また，同法によらずとも，個人情報データベース提供会社は，事業として，政府にその収集蓄積した膨大な個人情報を提供するようになっている。既に紹介したとおり，アメリカでは 1974 年に Privacy Act（PA）を制定し，政府保有の個人情報の取扱いについて，厳しい規制をかけてきた。ところが，テロや犯罪防止の目的で，民間の個人情報データベース提供会社で収集蓄積した個人情報を政府が有償で利用するようになっており，政府は Privacy Act の規制がないままに膨大な個人情報を利用している[77]。このように，個人情報産業と政府の複合体が従来のプライバシー保護体制の不備を突いた形で急成長してきている。政府保有の個人情報と民間部門保有の個人情報が相互に交換され，プロファイリングされた上で，これを政府が利用した場合，もはや利用できない個人情報はない状況まで進んでいく危険がある。

---

77) ロバート・オハロー・前掲注 72）193 頁以下。

日本においては，上記のように目立った動きはないものの，守秘義務がある金融機関も任意捜査や税務調査のための任意の協力要請に対しては，比較的広範な資料提供がなされているようである[78]。これらの資料提供は第三者提供の例外として個人情報保護法によっても規制されていない（法23条1号及び4号参照）。近時は，金融機関のATMに設置された監視カメラの映像が税務署の任意の調査に応じて提出されているという話も聞く。民間から政府への情報提供に関しては，本人に知らされることなく，民間が保有する金融情報等のセンシティブな情報の取得も行われているにもかかわらず，明確な規制が定まっていないことが最も問題であると考えられる。早急な規制作りが必要であると考える。

(3) 個別立法の必要性

上記のとおり，アメリカのプライバシー保護の現状は，日本に対する警鐘となるものである。しかし，参考にすべき点もある。個別立法の利点としては，誰が何を目的にどんな情報を取得・利用するかを絞り込むことで規制の必要性に応じたきめ細やかな立法が可能であることである。例えば，前述の Health Insurance Portability and Accountability Act of 1996（HIPAA）の適用対象は，①医療保険者（保険会社等），②医療情報処理者（標準化されていない医療情報を受け取り標準化されたフォームに加工する者等），③医療サービス提供者（医者，病院，薬剤師等）のみであり，かつ保護の対象となる情報は，HIPAA対象者（上記①から③）及びその業務委託者が保有または送信した個人識別可能な医療情報に限定されている。このような限定がされるのは，プライバシー問題は，同じ情報でも利用される背景によって保護の必要性や態様が異なるからである。氏名と電話番号といった一般的な個人情報でも，ストーカーがこれを入手して利用する場合とホテルが連絡の必要のために取得する場合とでは保護の必要性や態様が異なる。規制する場面，主体及び対象情報等を限定することで，時には刑事罰も含めて強力な規制を行ったり，またはよりゆるやかな規制を行ったりすることが可能となる。Children's Online Privacy Protection Act of 1998（COPPA）は，12歳以下の子供の情報をインターネットのウエブサイトで収集及び利用することを制限し，違反に対しては連邦取引委員会（FTC）が罰金を科すこともできるが，これは強力な規制をしている例である。さらに，Privacy Act，Video Privacy Protection Act

78) 「公的調査等と銀行の守秘義務」金法1482号6頁以下（1997年）。

及び Cable Communications Policy Act などは法律の規定に違反した場合に，損害額の立証をしなくとも法律で最低損害賠償額を定めている条項を有している。このように，個別立法では，ある程度損害を類型化して法律で損害賠償額を定めることができることも利点である。

民間部門において包括的な個人情報保護の法律を有する日本では，一応特定分野にとらわれず広く個人情報保護がなされる建前になっている。しかし，個人情報の商業利用や大規模利用が特に問題となる分野（金融，通信，医療等）においては，個人情報の集積・利用が進んでおり，一般的な法律の規制だけでは緩やかすぎ，不十分である。個別的状況に合わせてプライバシー保護を強化すべく個別立法の導入が検討されるべきである。この点，上記の分野を扱う民間部門に対しては，それぞれの分野毎に省庁が作成したガイドラインが定められている。しかし，その強制力は弱く，遵守状況にはばらつきがあるため個別立法による規制が望ましい。そして，かかる個別立法に際しては，企業に対するプライバシーの安全措置構築に向けた動機付けとして，法律で最低損害賠償額を定める手法を導入すべきである。現在の日本では，大規模な個人情報漏えいが起こっても裁判例上多くても一人あたり数万円という損害額しか認められておらず[79]，実務上，プライバシー侵害訴訟は費用倒れになるため泣き寝入りするケースが多い。これでは，企業は，真剣にコストをかけて個人情報保護のための安全措置を構築しようとは考えない。そこで，例えば金融機関の個人情報漏えいについては最低一人 10 万円の損害賠償義務を法定することで，裁判をしやすくなり，被害者救済と共に，個人情報漏えいが起こりやすい金融機関のプライバシー安全措置構築を進めることができると考える。

このように包括的な法律を有する日本においても，今後必要な分野において個別立法が必要である。

(4) 包括的な個人情報流通抑制の危険

これまで見てきたようにアメリカでは個人情報の高度の利用が進んでいる。プライバシーに関する問題を抱えながらアメリカが自主規制を中心とし包括的立法をしないのは，犯罪被害者報道規制に違憲判決を繰り返してきた連邦最高裁の厳しい態度に表れているように，個人情報の保護は，社会の公共財として

79) 東京地判平成 19 年 2 月 8 日判時 1964 号 113 頁など。

の情報流通を阻害するという側面を有しており，この点に関する主張が国民から相応の支持を集めていることにあると考えられる。

これに対して，日本では，個人情報保護法の制定後いわゆる過剰反応として過度に個人情報を秘匿する対応が，民間部門，公的部門を問わず見られた。公務員の懲戒処分情報が匿名になったり，JR 西日本の福知山線の事故に際して JR 西日本が個人情報保護法を理由に死傷者の搬送先などの情報提供を拒んだりした例がある。日本の個人情報保護法も情報流通をある程度意識しており，その第 1 条には目的として「個人情報の有用性に配慮しつつ，個人の権利利益を保護すること」が掲げられ，個人情報の有効活用も意識した表現になっている。また，同法は適用除外規定を有している（個人情報保護法 50 条列挙の報道目的利用，著述目的利用，学術研究目的利用，宗教活動目的利用及び政治活動目的利用）。それでも過剰反応は収まる気配を見せない[80)]。

日本の過剰反応事例を見ると，日本の個人情報保護の現状についてプライバシー意識が高く素晴らしいということは決してできない。日本には個人情報が社会の公共財という意識がないため極力流通させない方向に重点が置かれてしまっている。しかし，隣に住んでいる人がどんな人かわからず，事故の際に病院の入院患者も教えてもらえないような社会は本当に良い社会といえるだろうか。平松毅教授は，「個人情報保護法の目的は，個々人が交際する相手方に応じて，それぞれの人々に与える自己に関する個人情報を取捨選択することによって，すべての人々とよい人間関係を形成し，すべての人々と連帯することができるようにすることにある。そのためには，交際する相手方との機能不全を招く個人情報の流通を阻止しなければならない。これがプライバシーの権利なのである。」と述べている[81)]。人は一人では生きていけないのであって，共同社会で生活するにあたり当然に流通させるべき個人情報はある。ただし，正当な目的なく本人が嫌がる個人情報を流通させることに問題があるのである。日本においては，本人の同意がなくても流通させてよい個人情報が限定されすぎている。個人情報保護法は，全ての個人情報につき原則として流通を抑制する方

80) 日本弁護士連合会編『個人情報トラブル相談ハンドブック』26 頁以下（新日本法規，2007 年）。
81) 平松毅『個人情報保護　理論と運用』158 頁（有信堂，2009 年）。

向で規定されているのである。それは，個人情報保護法が包括的に個人情報の取扱いを定めた弊害といえる。

そして，流通すべき個人情報が流通しない社会は，人々との人間関係の形成が阻害され，連帯することが困難である。人間関係の形成が阻害されれば，個人が自由にさまざまな意見，知識，情報に接し，これを摂取する機会をもつことも妨げられる。例えば，ある人の連絡先がわからなければ，その人と交流して意見交換することができない。このように考えると，必要な個人情報の流通の確保は，表現の自由と密接不可分の関係にあり，民主主義社会における基本的原理を真に実効あるものとするために不可欠というべきである。最高裁法廷メモ訴訟判決（最判平成元年 3 月 8 日民集 43 巻 2 号 89 頁）も「憲法二一条一項の規定は，表現の自由を保障している。そうして，各人が自由にさまざまな意見，知識，情報に接し，これを摂取する機会をもつことは，その者が個人として自己の思想及び人格を形成，発展させ，社会生活の中にこれを反映させていく上において欠くことのできないものであり，民主主義社会における思想及び情報の自由な伝達，交流の確保という基本的原理を真に実効あるものたらしめるためにも必要であ」ると判示している。したがって，流通すべき個人情報が規制される社会は，民主主義の機能を低下させる危険を有しているのである[82)]。

流通すべき個人情報を流通させるためには，個人情報保護法の目的を解釈基準たるように明確化し，必要な個人情報が流通するように柔軟な解釈を可能とする規定を設けるべきである。さらに，柔軟な規定ゆえに予想される個人情報の取扱いをめぐる紛争を予防するために独立の監視機関を設置すべきである[83)]。

(5) パノプティコンにならないために

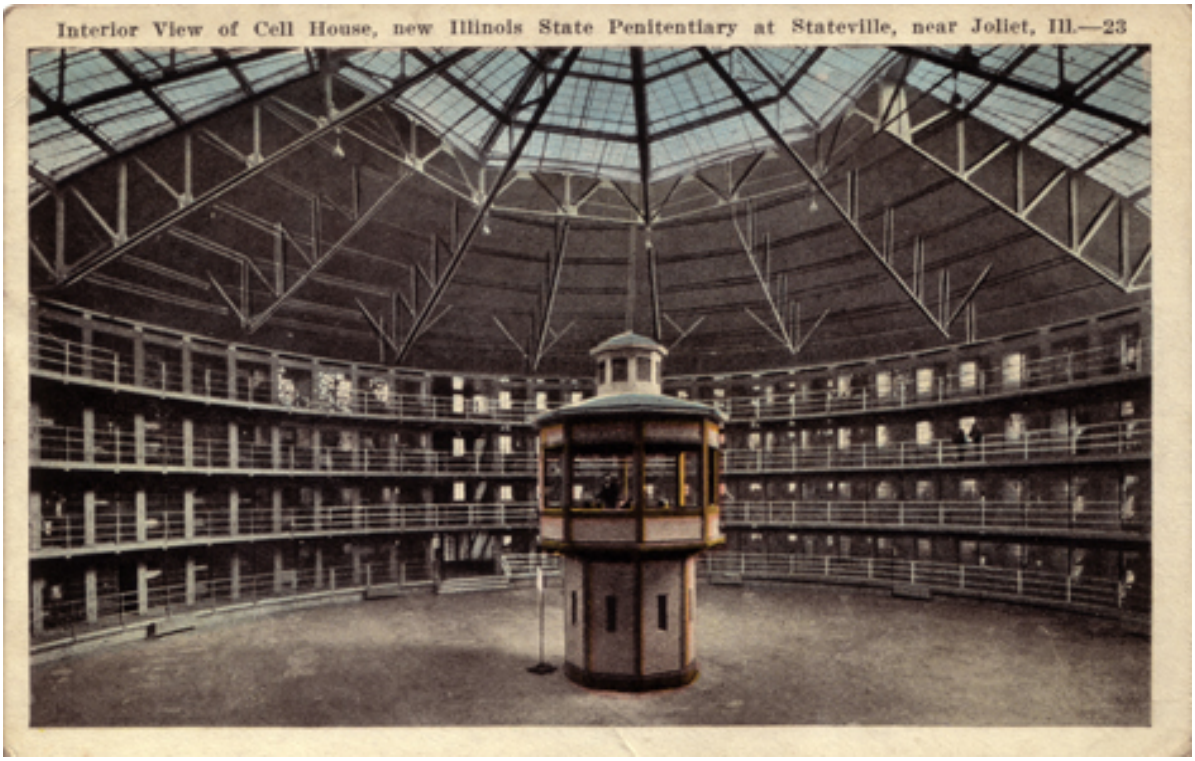
パノプティコンとは，独房が円形に配置され中心に監視所が設けられた刑務所の形式である。私が受講したプライバシーの授業で，プライバシーのない社会の比喩としてその写真が示された。

---

82) 佐藤幸治教授も「個人情報保護法制を自己完結的にとらえ，その運用を法技術論の次元でのみ行うと，公共的性質の情報も出なくなり，何よりも自由な情報流通（表現の自由）を阻害してしまいます。」と述べている（「個人情報保護，自己情報コントロール権の現状と課題」NBL912 号 21 頁（2009 年））。

83) 詳細な提言として平松・前掲注 81）153 頁以下，及び日弁連・前掲注 80）27 頁以下参照。

図 1：パノプティコン。 <http://www.hks.harvard.edu/sdn/sdnimages/images.panopticon.jpg> （2010 年 3 月 23 日最終アクセス）。



中心の監視所を政府，独房を個々の国民ととらえると，現在の日本の個人情報の取扱いが向かっている将来の姿にも見える。すなわち，国民間では個人情報の流通が抑制され，中央の政府だけが国民の個人情報を取得・利用して監視するという状況である。

日本では，既に述べたように国民間での個人情報の流通が抑制され民主主義社会に対する危険な状況が存在する。そして，中央の政府が大規模に国民の個人情報を取得・利用できる状況も実現しつつある。すなわち，住民基本台帳ネットワークの稼働により，国民の個人情報をデータベース化する基礎が整った。加えて，納税者番号制度の早期導入が検討されており，個人の収入支出といった情報も漏れなく把握されようとしている。また，監視カメラは街中に増加しつつあり，これと顔貌認識システムを組合わせて，特定人の行動を追跡することが技術的に可能となりつつある。自動車での行動については，すでに自動車ナンバー自動読み取り装置（N システム）が主要な道路に設置されており，特に犯罪の嫌疑のない車両についても警察において自動的に記録されている。さらに，アメリカの状況にあるようにクレジットカード利用履歴やウエブサイトの

閲覧情報など民間が保有する大量の情報がテロ防止といった名目で政府に提供される恐れもある。

棟居快行教授は，住基ネットによるプライバシー侵害について「自分以外の存在が，自分以上にさまざまの個人情報を集積し分析しているかもしれないという不安が，個人の日常を萎縮させ，自由で自律的な存在から，単に行政サービスに依存する他律的な存在へと人を堕落させうるのである。」と述べる[84]。そして，個人の人格的自律は，個人の利益だけの問題ではなく，社会公共の問題でもある。佐藤幸治教授は，「プライヴァシーは個人の利益に役立つのみならず，共有的価値（common value），公共的価値（public value），および集合的価値（collective value）にもかかわっていることに留意する必要がある」とし，「プライヴァシーの権利は，自由な個人のあり方を規定するのみならず，多元的で，寛容な社会のあり方をも規定する。また，プライヴァシーの権利は，民主的な政治システムにとっても不可欠のものである。」と述べる[85]。また，平松教授は，個人情報保護法について「この法律を制定した目的は，個人の人格権を保護することにあるが，同時にそれは公益でもあることに注意する必要がある。すなわち，われわれは，国や他人が自己に関してどのような情報を有しているかを予測することができない場合には，われわれは，国による評価または他人との人間関係の形成に不安を感じるから，自己の個人情報を開示しないようにしたり，自己の行動を自粛することによってありうべき不利益に対処しようとするであろう。…（略）…しかし，民主主義は，個々人が自己の良心に基づいて自律的に判断し，行動する自律した個人から構成されることにより健全に機能する以上，国民が，自己に関する情報がどこで把握され，どう使用されているかに不安を抱く社会では，国民は自己の行動を自主規制することにより，民主主義を機能不全に陥らせる危険があるからである。」と述べている[86]。このように，国家による個人情報の収集・利用は民主主義社会に対する影響が重大である。

しかし，この問題点に対する日本社会の危機意識は低い。アメリカは，プライバシー権が最初に提唱され，これに対する問題意識も昔から高かった国であるが，政府による監視活動も活発になされてきた国である。例えば，FBI は公民

84) 棟居快行編『岩波講座　憲法 2　人権論の新展開』220-221 頁〔棟居快行〕（岩波書店，2007 年）。
85) 佐藤幸治『現代国家と人権』518 頁（有斐閣，2008 年）。
86) 平松・前掲注 81）154 頁。

権運動指導者でノーベル平和賞を受けたキング牧師を盗聴し，その男女関係をネタにキング牧師の活動をやめさせるため脅迫を行っていたことはロースクールのテキストにも紹介されている著名な事実である。アメリカの状況を見れば，国家によるプライバシー侵害が，過去のものでも遠い未来のものでもなく，しかもひとたび国家権力がプライバシー侵害を始めたら民間よりずっと重大な影響を与えることがわかる。そして，個人情報の流通が抑制されている日本は，アメリカよりも危険なパノプティコン状態に向かっていることが認識されなければならない。